REVERSINGLABS

DATA SH EE T

TitaniumScale 엔터프라이즈 스케일 파일 분석

포괄적인 파일 레벨 위협 분류 및 가시화

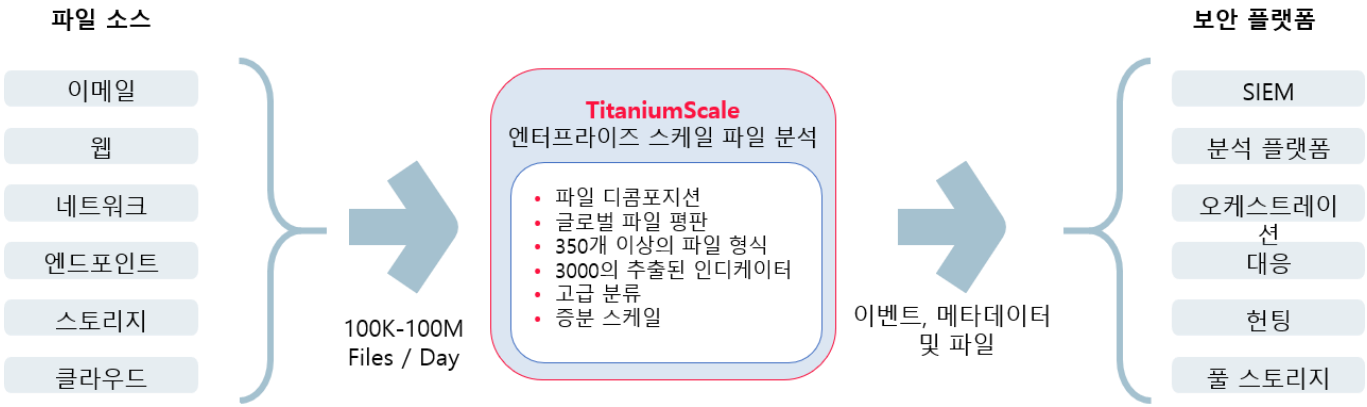
주요기능

- **실시간 파일 심층분석** - 파일 실행없이 일단위 수백만 개 이상의 파일분석 확장가능
- **넓은 커버리지** - 350개 이상의 압축해제 파일 및 3500개 이상의 파일형식 식별지원
- **다양한 인풋을 통한 파일수집 –** 리버싱랩스 및 써드파티 제품의 자동화된 제출방식을 통해 수집
- **사용자 지원 YARA 규칙 매칭**
- **검색가능한 추출 파일 프로파일** - 파일의 콘텍스트 또는 콘텐츠를 통한 지원
- **인프라스트럭쳐 증분 스케일** - 고객 사용량과 용량 요구사항 충족
- **프로그래밍 가능한 인프라스트럭쳐** - 위협 식별, 분석플랫폼, 헌팅, 및 소프트웨어 검증 지원
- **자동화 운영의 원활한 연동** - SIEM, 분석플랫폼, 파일 컬렉션

TitaniumScale은 대용량 파일을 실시간으로 프로파일링하고 분류하여 위협 상관관계 탐색, 헌팅 및 대응을 지원하기 위한 고급 분석 플랫폼 관련 데이터를 생성합니다. 기존의 멀웨어 제품은 탐지되지 않은 파일을 굿웨어로 인식 또는 간과하며 멀웨어 탐지에 포커스합니다. 탐지를 회피하는 멀웨어가 증가함에 따라 탐지되지 않은 파일을 프로파일링, 트래킹 및 관련성 부여의 필요성은 임펙트를 제한하고 침해와 사고 해결방안을 가속화하기 위해 필수적입니다. 인텔리전스 데이터는 지루하고 고비용을 요구하는 사후 침해복구와 멀웨어 탐지 사이의 가시성 갭을 축소시킵니다.

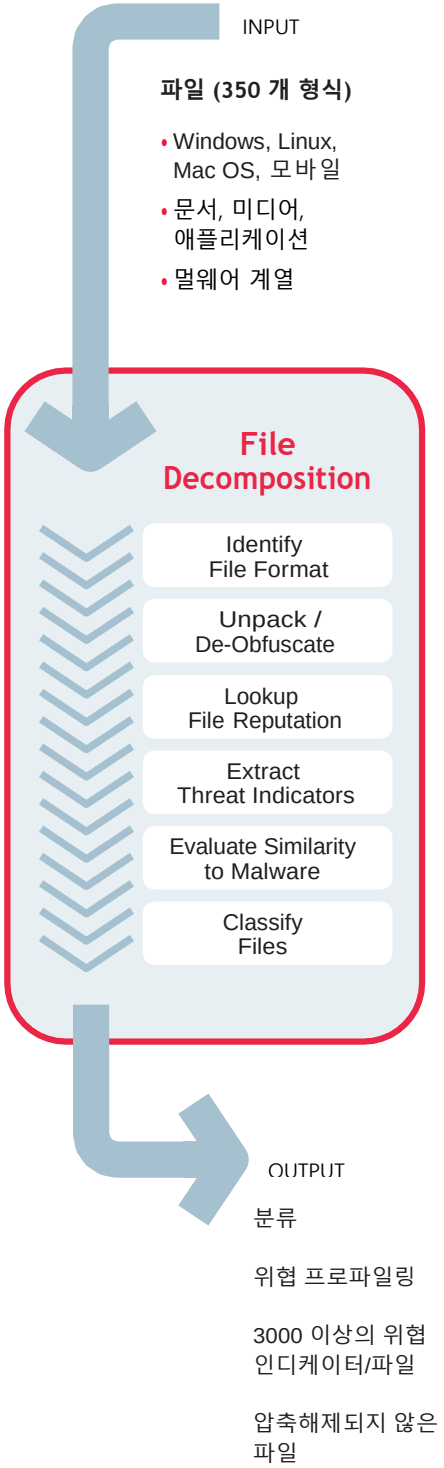
TitaniumScale은 웹트래픽, 이메일, 파일전송, 엔드포인트 및 스토리지 출처의 수백만개 파일에 대한 포괄적인 기업 평가를 지원합니다. 이 솔루션은 리버싱랩스의 고유한 파일 디콤포지션 기술을 이용하여 상세 메타데이터를 추출하고 글로벌 평판 콘텍스 추가와 위협을 분류합니다. TitaniumScale은 이메일, 게이트웨이, 인트루젼 탐지, 시스템 방화벽 및 그 외 장치 등의 엔터프라이즈 보안 인프라스트럭처에 설치된 솔루션과 연동하여 자동으로 파일을 수집합니다.

그 결과, 업계를 선도하는 SIEM, 오케스트레이션, 분석 플랫폼에 반영되어 가시성과 데이터를 분석도구에 제공하고 어드밴스드 헌팅 전략지원과 고급정책 이행의 강제를 지원합니다.



TitaniumScale 사용사례

파일분류 – 실시간 파일 검사와 분류로 멀웨어 가시성의 갭을 축소시킵니다.
대응 가속화 – 기존의 파일속성을 검색하여 위협을 탐지합니다.
사용자 지정 분류 – YARA 규칙을 이용한 엔터프라이즈급 스케일의 타겟 멀웨어 식별을 수행합니다.
애플리케이션 검증 – 배포 전에 설치를 체크하고 패키지를 업데이트합니다.



파일 디콤포지션

TitaniumScale은 파일에서 광범위한 내부 평판 및 분류 정보를 가져오고, 인텔리젼스를 SIEM, 고급 분석 및 빅테이터 플랫폼에 익스포트 할 수 있습니다.

리버싱랩스의 파일 디콤포지션 기술을 사용하여 파일에서 실시간으로 상세 내부 인디케이터와 크리티컬 콘텍스트를 추출합니다.

파일 디콤포지션은 샌드박스가 아닌 자동화된 정적분석을 사용하여, 다양한 플래폼의 파일, 애플리케이션 및 멀웨어 툴킷은 밀리세컨드 단위로 처리됩니다.

시스템은 재귀적으로 파일 압축해제, 평판정보 조회, 알려진 멀웨어와 기능적 유사성 확인, 내부 인디케이터 밀리세컨드 내에 추출 및 파일의 위협레벨과 심각도 분류 등 다양한 작업을 수행합니다.

모든 파일은 70억개 이상의 굿웨어 및 멀웨어 파일을 보유하고 있는 리버싱랩스의 포괄적인 파일 평판 데이터베이스를 통해 검사합니다. 검사결과는 현재 및 과거 이벤트의 응답으로 SIEM과 분석 플랫폼을 통해 각 파일별 특성화하여 제시합니다.

주요 기능

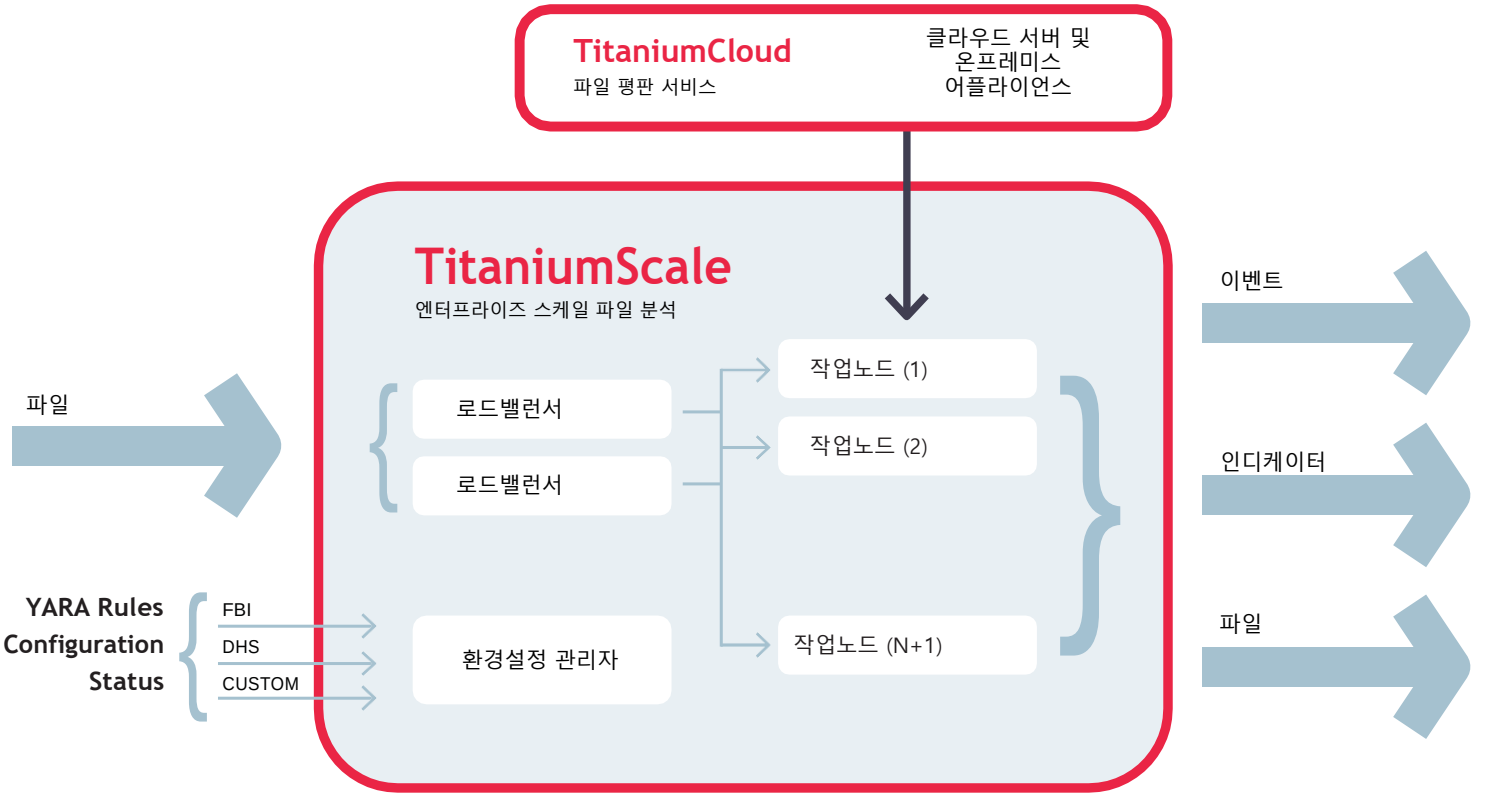
- **속도** - 대용량 처리 실시간 지원을 위한 밀리세컨드 내 파일 목록화
- **커버리지** - 350개 이상의 파일형식을 처리되고 3500개 이상의 파일형식을 다양한 플랫폼 애플리케이션 및 멀웨어 계열을 통해 식별
- **뎁스** - 재귀적 압축해제와 파일 당 3000개 이상의 인디케이터 추출
- **평판** - 업계 가장 포괄적인 굿웨어/멀웨어 데이터베이스를 통한 파일 검사
- **분류** - 리버싱랩스 및 사용자 지정 YARA 규칙을 지원하는 고급 규칙을 통한 분석

확장 가능형 아키텍처

TitaniumScale은 유연한 증분형 확장이 가능한 클러스터 아키텍처를 사용하여 물리적 환경 및 클라우드 환경에서 배포 또는 중앙화된 파일 처리를 지원합니다.

TitaniumScale 은 다음과 같이 구성되어 있습니다:

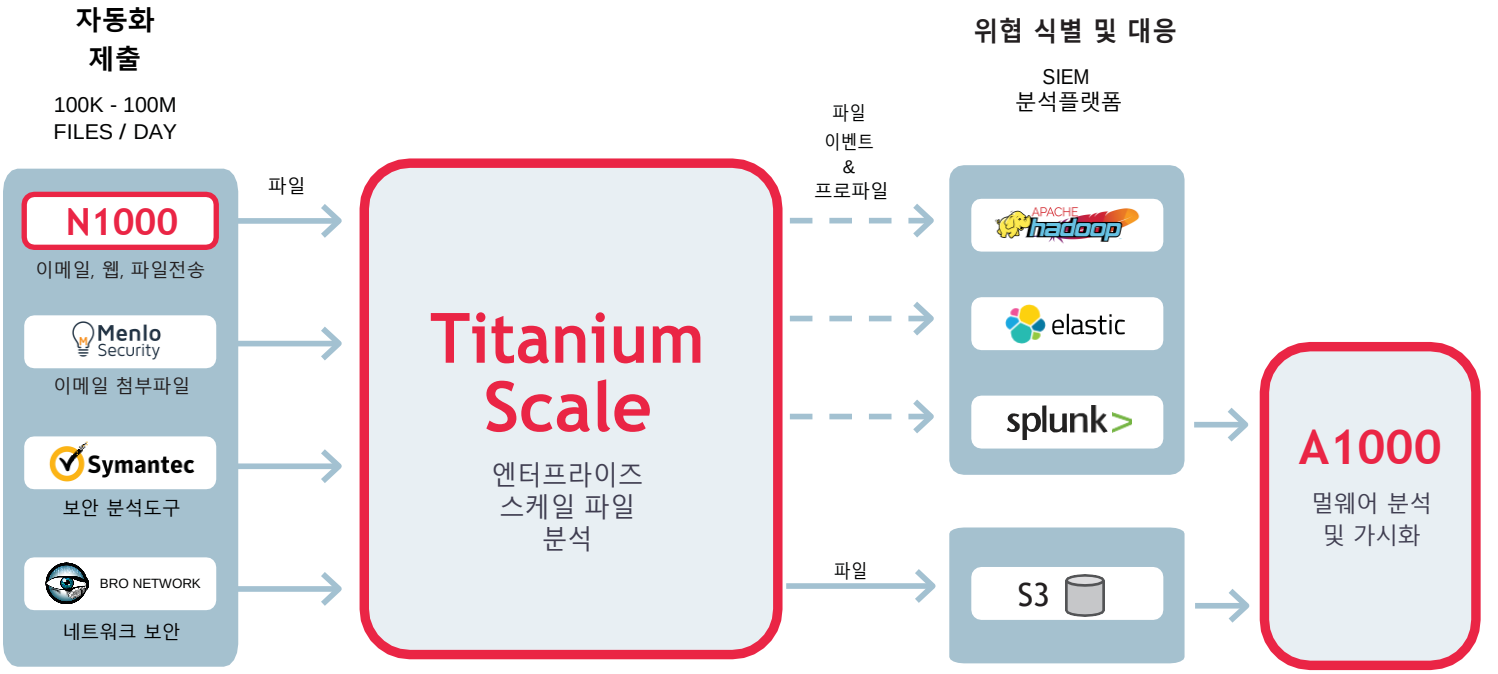
- **작업노드** - 물리적 서버 또는 가상서버의 클러스터로 실제 파일 평가를 수행하고 N+1 리던던시를 지원
- **로드 밸런서 허브** - 파일을 처리하기 위해 작업노드를 전달하는 서버와 예비서버(옵션)
- **컨트롤 매니저** - 환경설정을 관리하고 TitaniumScale 클러스터 상태를 모니터링하는 서버
- **TitaniumCloud 파일 평판** - 클라우드 또는 온사이트 어플라이언스 환경에서 알려진 굿웨어 및 멀웨어를 식별하고 정보를 제공하는 서비스



구축 사례

대규모 금융조직에서 TitaniumScale을 사용하여 상세 파일 프로파일링과 분류 정보를 획득합니다. 해당 기업은 결과 인텔리전스 정보를 분석 플랫폼에 반영하여 위협을 식별하고 사고에 신속하게 대응합니다. TitaniumScale 을 20개 데이터 센터에 디플로이하여 이메일, 웹, 파일 전송 트래픽에서 파일을 추출하고 자동으로 분산 TitaniumScale 클러스터에 제출합니다. 획득한 프로파일링 정보는 해당 파일의 복사본을 링크한 URL을 포함합니다. 이를 통해 추가 분석이 가능합니다.

리버싱랩스의 A1000 멀웨어 분석 어플라이언스는 상세 분석에 대한 접근과 이에 대한 가시화를 제공합니다. 결과적으로 고객사는 기존의 멀웨어 탐지 기술이 찾지 못하는 위협을 식별하고 상관관계 탐색 및 솔루션 제공을 가속화할 수 있습니다.



REVERSINGLABS
Korea Sales: 02.538.9225
briankim@reversinglabs.co.kr